日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年　８月２０日

出 願 番 号
Application Number: 平成１１年特許願第２３３８１５号

出 願 人
Applicant (s): 松下電器産業株式会社

２０００年　６月　９日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号　出証特２０００－３０４４８５６

【書類名】　特許願

【整理番号】　2022510372

【提出日】　平成11年 8月20日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/32

H04L 12/14

H04L 9/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　勝田　昇

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　河田　浩嗣

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　茨木　晋

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　舘林　誠

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　原田　俊治

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【プルーフの要否】　不要

【書類名】　明細書

【発明の名称】　データ再生装置および鍵記憶装置および情報埋め込み確認方法および鍵使用履歴記録方法および透かし情報埋め込み装置およびその検出装置

【特許請求の範囲】

【請求項１】　暗号化されたデータを復号する復号鍵記憶手段と前記復号鍵の読み取りを許可する読み取り許可手段と鍵の読み出し実績を記憶する読み出し履歴記憶手段を具備し、

前記復号鍵は、鍵の読み出し有効期間情報を含み、前記読み取り許可手段は、外部より読み取り要求時に要求時の時刻情報を含む鍵要求信号を受け取り、前記時刻情報の示す時刻が前記読み出し履歴情報の最も新しい時刻よりも後の時刻であることと鍵の読み出し有効期間内にあることを確認して読み取り許可を与えることを特徴とする鍵記憶装置。

【請求項２】　さらに、履歴記憶手段は、履歴情報に加えてそのデータの改ざんが検出可能な改ざん検出コードを生成記録することを特徴とする請求項１記載の鍵記憶装置。

【請求項３】　さらに、読み取り許可手段は、履歴情報につけられた改ざん検出コードにより、履歴情報に改ざんがないことを確認して読み取り許可を与えることを特徴とする請求項２記載の鍵記憶装置。

【請求項４】　履歴記憶手段は、所定の記憶容量を持ち、読み取り許可手段は、履歴記憶手段に記憶された履歴情報が履歴情報記憶手段の記憶容量に達した時、鍵読み取りを不許可として制御することを特徴とする請求項１記載の鍵記憶装置。

【請求項５】　復号鍵取得手段と前記取得した復号鍵に基づき入力データを解読処理する復号処理手段と復号されたデータに電子透かしを埋め込む電子透かし埋め込み手段と本装置の識別コードを記憶する機器識別コード記憶手段を具備し、

復号鍵取得手段は、復号鍵取得時、読み出し時点の鍵読み出し時刻を保持し、電子透かし埋め込み手段は、機器識別コードおよび前記鍵読み出し時刻を埋め込み情報として再生データに埋め込むことを特徴とするデータ再生装置。

【請求項６】　さらに、復号鍵読み取り手段は、鍵を読み出す鍵記憶装置の識別番号を復号鍵とともに読み出すとともに保持し、電子透かし埋め込み手段は、鍵読み出し装置識別番号を埋め込み情報として埋め込むことを特徴とする請求項５記載のデータ再生装置。

【請求項７】　さらに復号鍵鍵取得手段は、読み出し時刻および機器識別コードを含む鍵読み出し履歴信号を生成し鍵記憶手段に伝送することを特徴とする請求項５記載のデータ再生装置。

【請求項８】　暗号化されたデータの再生用鍵を記憶する鍵記憶手段と前記鍵記憶手段から再生用鍵データを読み出して再生処理するデータ再生手段からなり、データ再生手段と鍵記憶手段は、着脱可能な接続がなされ、鍵記憶手段は、データ再生手段が再生鍵を読み出したとき、データ再生装置の機器識別コードと読み出し時刻を含む鍵読み出し履歴を記録し、データ再生手段は、再生鍵に基づき再生する再生データに、再生鍵取得時刻および機器識別コードを透かし情報として埋め込むことを特徴とするデータ再生装置。

【請求項９】　時刻情報および機器識別コードを透かし情報として埋め込んだデータ中より埋め込まれた透かし情報検出し、データへの情報埋め込み履歴データベースより前記検出処理で検出できた埋め込み情報と照合処理することを特徴とする埋め込み情報確認方法。

【請求項１０】　鍵の読み出し処理が行われた鍵読み出し時刻読み取り、最も近い以前の時刻に記録された時刻間を鍵未使用期間を意味するデータを記録し、次に前記鍵読み取り時刻を含む鍵読み取り情報を記録し、読み取られた鍵使用終了時、その終了時刻を記録することを特徴とする鍵使用履歴記録方法。

【請求項１１】　埋め込みパターンを各映像フレーム毎への埋め込み値列に変換する埋め込み列生成手段と各埋め込み列に基づき各フレームに情報を情報埋め込み手段からなり、埋め込み列生成手段は、埋め込みパターンを各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと埋め込みパターンを１ビットずつ複数フレームにわたって同じ値を埋め込むことにより埋め込みビット数の複数倍のフレーム数を用いて埋め込む長周期埋め込むパターンを混在させた埋め込みパターンを生成することを特徴とする透かし情報埋め込み

装置。

【請求項１２】　請求項１１記載の透かし情報埋め込み装置により透かし情報を埋め込まれたデータから埋め込み情報を検出するものであって、各フレームから埋め込みパターンを検出するフレーム内埋め込み情報検出手段と前記フレーム内埋め込み手段が検出パターンより、短周期埋め込みされたビットに対応するパターンに基づき埋め込みパターンを算出する短周期埋め込みパターン検出手段と長周期埋め込みビットを参照して埋め込みパターンを算出する長周期埋め込みパターン検出手段からなる透かし情報検出装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データへのアクセス権を有効期間ないだけ許すアクセス管理およびそのデータが著作物である場合の不正使用の検知や防止を実現可能なデータ再生装置および鍵記憶装置および埋め込み情報確認方法および鍵使用履歴記録方法に関する。

【０００２】

【従来の技術】

従来のデータ再生装置は、ディジタルビデオディスクプレイヤー（DVDプレイヤー）などがある。これは、DVDビデオに格納されたデータを著作権保護対策を行わないような機器で再生できないように、ディスクにかかれるデータを暗号化して記録してあり、正規に鍵を付与されたプレイヤーのみ再生が可能になるものである。一般のDVDプレイヤーの場合、この再生用に機器に与えられた鍵は、固定的に与えられている。一方、映画の劇場への電子配信や航空機内のビデオサービスにおいては、劇場で公開される以前のものなどがあり、その再生できる期間を制御できるものが望まれている。このようなデータへのアクセスについて有効期限を設ける方法としては、鍵に有効期限を設け、鍵を利用する際に現在時刻を検出し、その時刻が有効期限内にあるかどうかによって鍵の利用を制御することで有効期間内だけ鍵を有効にすることができる。

【０００３】

また、データの再生に際して、その再生を行った機器の識別番号等を透かし情報として埋め込むことにより、再生データを不正にコピーして販売するなどをされた場合にその原因となった再生機器を突き止めることが考えられている。

【０００４】

【発明が解決しようとする課題】

しかるに、従来の再生装置においては、有効期限を判定する際の正確な時刻を検出することが課題となっている。すなわち、現在時刻を検出する方法として再生装置内部に時計機能を持たせることが考えられるが、時計の誤差等を修正する機構を設けた場合、不正に時計を操作して再生装置内の時計を都合のよい時刻に変更されてしまう問題があった。同様に外部に時計を設けてそれを検出する場合もその時計への不正な操作が行われる問題があった。

【０００５】

また、再生データに透かし情報を埋め込んだ場合、それを正しく検出する必要があるが、埋め込みデータが増えた場合、そのすべての情報を間違いなく検出することが困難になる問題があった。たとえば、映像信号中に機器の識別コードを埋め込んで追跡する場合、識別コードを正しく読まなくてはならないが、

映像信号に情報が埋め込まれていることがわからない程度に情報を埋め込める量は、少なく１フレーム内に埋め込みきれず数フレームに及んだ場合等には、そのうちの数フレームを抜き取るだけで正しく検出できない。また、検出結果が正しさを保証できる手段がなかった。

【０００６】

以上のような問題に鑑み本発明の目的は、時刻情報を不正に操作して鍵有効期間外で鍵のアクセスによる不正なデータ再生を防止し、また不正なコピーに対してより高い追跡性を実現する再生装置および鍵記憶装置を提供することである。

【０００７】

【課題を解決するための手段】

以上の課題を解決するために、本発明は、暗号化されたデータを復号する復号鍵記憶手段と前記復号鍵の読み取りを許可する読み取り許可手段と鍵の読み出し実績を記憶する読み出し履歴記憶手段を具備し、前記復号鍵は、鍵の読み出し有

効期間情報を含み、前記読み取り許可手段は、外部より読み取り要求時に要求時の時刻情報を含む鍵要求信号を受け取り、前記時刻情報の示す時刻が前記読み出し履歴情報の最も新しい時刻よりも後の時刻であることと鍵の読み出し有効期間内にあることを確認して読み取り許可を与える鍵記憶装置の構成である。

【０００８】

また、さらに履歴記憶手段は、履歴情報に加えてそのデータの改ざんが検出可能な改ざん検出コードを生成記録する鍵記憶装置の構成である。

【０００９】

また、さらに、読み取り許可手段は、履歴情報につけられた改ざん検出コードにより、履歴情報に改ざんがないことを確認して読み取り許可を与える鍵記憶装置の構成である。

【００１０】

また、履歴記憶手段は、所定の記憶容量を持ち、読み取り許可手段は、履歴記憶手段に記憶された履歴情報が履歴情報記憶手段の記憶容量に達した時、鍵読み取りを不許可として制御する鍵記憶装置の構成である。

【００１１】

また、復号鍵取得手段と前記取得した復号鍵に基づき入力データを解読処理する復号処理手段と復号されたデータに電子透かしを埋め込む電子透かし埋め込み手段と本装置の識別コードを記憶する機器識別コード記憶手段を具備し、復号鍵取得手段は、復号鍵取得時、読み出し時点の鍵読み出し時刻を保持し、電子透かし埋め込み手段は、機器識別コードおよび前記鍵読み出し時刻を埋め込み情報として再生データに埋め込むデータ再生装置の構成である。

【００１２】

さらに、復号鍵読み取り手段は、鍵を読み出す鍵記憶装置の識別番号を復号鍵とともに読み出すとともに保持し、電子透かし埋め込み手段は、鍵読み出し装置識別番号を埋め込み情報として埋め込むデータ再生装置の構成である。

【００１３】

さらに復号鍵鍵取得手段は、読み出し時刻および機器識別コードを含む鍵読み出し履歴信号を生成し鍵記憶手段に伝送するデータ再生装置の構成である。

【００１４】

また、暗号化されたデータの再生用鍵を記憶する鍵記憶手段と前記鍵記憶手段から再生用鍵データを読み出して再生処理するデータ再生手段からなり、データ再生手段と鍵記憶手段は、着脱可能な接続がなされ、鍵記憶手段は、データ再生手段が再生鍵を読み出したとき、データ再生装置の機器識別コードと読み出し時刻を含む鍵読み出し履歴を記録し、データ再生手段は、再生鍵に基づき再生する再生データに、再生鍵取得時刻および機器識別コードを透かし情報として埋め込むデータ再生装置の構成である。

【００１５】

時刻情報および機器識別コードを透かし情報として埋め込んだデータ中より埋め込まれた透かし情報検出し、データへの情報埋め込み履歴データベースより前記検出処理で検出できた埋め込み情報と照合処理する埋め込み情報確認方法である。

【００１６】

また、鍵の読み出し処理が行われた鍵読み出し時刻読み取り、最も近い以前の時刻に記録された時刻間を鍵未使用期間を意味するデータを記録し、次に前記鍵読み取り時刻を含む鍵読み取り情報を記録し、読み取られた鍵使用終了時、その終了時刻を記録する鍵使用履歴記録方法である。

【００１７】

また、埋め込みパターンを各映像フレーム毎への埋め込み値列に変換する埋め込み列生成手段と各埋め込み列に基づき各フレームに情報を情報埋め込み手段からなり、埋め込み列生成手段は、埋め込みパターンを各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと埋め込みパターンを１ビットずつ複数フレームにわたって同じ値を埋め込むことにより埋め込みビット数の複数倍のフレーム数を用いて埋め込む長周期埋め込むパターンを混在させた埋め込みパターンを生成する透かし情報埋め込み装置の構成である。

【００１８】

また、透かし情報を埋め込まれたデータから埋め込み情報を検出するものであって、各フレームから埋め込みパターンを検出するフレーム内埋め込み情報検出

手段と前記フレーム内埋め込み手段が検出パターンより、短周期埋め込みされたビットに対応するパターンに基づき埋め込みパターンを算出する短周期埋め込みパターン検出手段と長周期埋め込みビットを参照して埋め込みパターンを算出する長周期埋め込みパターン検出手段からなる透かし情報検出装置もの構成である。

【００１９】

【発明の実施の形態】

以下、本発明の実施の形態について、添付図面を参照して説明する。

【００２０】

（実施の形態１）

図１は、本発明の実施の形態１のデータ再生装置および鍵記憶装置を含むシステムの構成図である。図１において、１は、鍵の生成などを行う鍵管理部、２は、鍵管理部１が生成した鍵を記憶する鍵記憶装置で、鍵管理部で生成した再生装置鍵記憶部３とその有効期間記憶部４、鍵の読み取り履歴記憶部５および鍵記憶装置識別コード記憶手段６からなり、７は、データ再生装置であり、データ再生装置識別コード記憶部８と鍵複号処理部９、再生処理部１０および電子透かし埋め込み処理部１１からなり、１２は、時計、１３は、暗号化データおよびその暗号化鍵を再生装置鍵で暗号化されたものが記憶された記録メディア（たとえば、ＤＶＤ）、１４は、鍵暗号化手段、１５は、データ暗号化手段である。

【００２１】

以上のような構成において以下にその動作を説明する。鍵管理部１は、データ再生装置毎の再生装置鍵を生成し、鍵記憶装置２の再生装置鍵記憶部３とその有効期間記憶部４へ記録する。また、映画などのコンテンツデータを記録メディアに書き込み者へ再生装置鍵およびその有効期間を送る。その再生装置鍵は、鍵暗号化手段１４へ入力される。コンテンツデータは、コンテンツ鍵で亜データ暗号化処理部１５で暗号化され記録メディア１３に記録される。また、この時のコンテンツ鍵を再生装置鍵を用いて暗号化処理手段１４で暗号化したものを記録メディア１３にあわせて記録する。以上のように、コンテンツデータをコンテンツ鍵で暗号化した暗号化コンテンツデータとそのコンテンツ鍵を再生装置鍵で暗号化

した暗号化コンテンツ鍵が記録された記録メディアが生成され、再生装置７へ送られる。これらの処理は、一般のＤＶＤビデオの映画タイトル等の生成において行われているため、処理の概略を示したが、複数の再生装置へ配布可能にするために、通常は、その配布先の再生装置鍵でコンテンツ鍵を暗号化したものを複数記憶させておく。

【００２２】

図１に戻って、記録メディア１３のデータを鍵記憶装置２およびデータ再生装置７で再生する処理を説明する。データ再生装置７は、記録メディア１３を再生する場合、接続された鍵記憶装置２から再生装置鍵を読み取り、それを鍵複号処理部９に入力し、記録メディア１３より暗号化コンテンツ鍵を読み出し鍵復号処理部９に入力して復号し、その復号されたコンテンツ鍵を再生処理部１０へ入力する。再生処理部１０は、暗号化コンテンツデータをコンテンツ鍵を用いて暗号解読したのち、そのデータの内容にしたがって再生処理する。たとえば、ＭＰＥＧ２フォーマットで圧縮されたビデオデータの場合、ＭＰＥＧ２デコーダ処理され、映像信号に再生される。データ再生装置７が、再生装置鍵を読み取る際、時計１２より時刻情報を取得し、再生装置識別コードとともに時刻情報を鍵記憶装置２へ送る。この際、再生するコンテンツデータにコンテンツ識別情報がある場合は、コンテンツ識別情報も送る。鍵記憶装置２は、送信されてきた時刻情報と有効期間記憶部４の有効期間を比較し、有効期間内であれば再生装置鍵記憶部３内の再生装置鍵と鍵記憶装置識別コード記憶部６内の鍵記憶装置識別コードをデータ再生装置７へ送る。そして、データ再生装置７から送られたきた時刻情報、再生装置識別コード、コンテンツ識別コードを履歴情報として履歴情報記録部５に記録する。次に、データ再生装置７は、鍵読み取り時刻情報と再生装置識別コードおよび鍵記憶装置識別コードを埋め込み情報として電子透かし情報埋め込み処理部１１で再生データに埋め込み処理する。

【００２３】

鍵記憶装置２とデータ再生装置７間の処理の詳細を図２から図６を用いて説明する。図２は、鍵記憶装置２の構成図である。図２において、２０１は、入出力インターフェイスでデータ再生装置７あるいは、鍵管理部１と接続される場合に

用いられ、２０２は、制御部、２０３は、履歴情報記憶部、２０４は、再生装置鍵記憶部、２０５は、有効期間記憶部、２０６は、鍵記憶部再生装置間鍵記憶部、２０７は、鍵記憶装置識別コード記憶部、２０８は、コンテンツ識別コード記憶部、２０９は、再生装置識別コード記憶部、２１０は時刻情報記憶部である。図３は、データ再生装置７の構成図である。図３において、３０１は、鍵記憶装置２との入出力インターフェイス部であり、図２の入出力インターフェイス部２０１と接続され、３０２は、制御部、３０３は、鍵記憶装置識別コード記憶部、３０４は、再生装置識別コード記憶部、３０５は、鍵取得時刻記憶部、３０６は、鍵復号処理部、３０７は、再生処理部、３０８は、電子透かし情報埋め込み処理部、３０９は、コンテンツ識別コード記憶部、３１０は、鍵記憶部再生装置間鍵記憶部である。

【００２４】

以下動作を説明する。鍵記憶装置２とデータ再生装置７は、入出力インターフェイス２０１および３０１で接続される。たとえば、鍵記憶装置２は、スマートカードのようなＣＰＵつきのメモリカードで実現でき、この場合ならメモリカード接点とICカードリーダが入出力インターフェイス２０１、３０１にそれぞれ対応する。接続されると制御部２０２および３０２間の制御手順にしたがって鍵の読み取りが行われる。図４は、再生装置鍵の取得処理の処理手順の説明図である。同図において、４０１は、コンテンツ識別コード取得処理、４０２は、時刻情報取得処理、４０３は、鍵リクエスト送信処理、４０４は、最新読み取り時刻との比較処理、４０５は、鍵有効期間確認処理、４０６は、履歴書き込み処理、４０７は、鍵配送処理である。制御部２０２と３０２間の送信データは、鍵記憶部再生装置間鍵記憶部２０６および３１０にある共有されている鍵記憶部再生装置間鍵で暗号化通信される。暗号復号化処理は、制御部２０２および３０２でソフト的に行うことが可能である。まず、記録メディア１３がデータ再生装置７にかけられたとき、制御部３０２は、記録メディア１３内にあるコンテンツ識別コードを読み取りコンテンツ識別コード記憶部３０９に記憶する。次に時計１２より、時刻情報取得４０２で時刻情報を読み出し、鍵取得時刻記憶部３０５に記憶する。次に、鍵リクエスト送信処理４０３で鍵をリクエストコマンドに鍵取得時刻

記憶部３０５の時刻情報と再生装置識別コード３０４内の再生装置識別コードおよびコンテンツ識別コード３０９内のコンテンツ識別コードをつけて送信する。次に、制御装置２０２は、コンテンツ識別コード記憶部２０８再生装置識別コード記憶部２０９、時刻情報記憶部２１０にそれぞれ送られてきた値を記憶して、最新読み取り時刻との比較処理４０４で履歴情報記憶部２０３の最新の時刻と時刻情報記憶部２１０の値を比べ、最新情報よりも時刻情報が以後の時刻を示していれば処理が成功し、もしそうでなければ、以後の処理を直ちに中止する。つぎに鍵有効期間確認処理４０５で、制御部２０２は、時刻情報２１０の時刻が有効期間２０５内に示された有効期間内にあれば、処理が成功したとし、そうでなければ以後の処理を直ちに中止する。そして、履歴書き込み処理４０７で、コンテンツ識別コード記憶部２０８、再生装置識別コード記憶部２０９、時刻情報記憶部２１０の情報を履歴情報として記憶する。ただし、履歴書き込むに失敗すれば、以後の処理を直ちに中止する。

【００２５】

以上の３つの処理が成功すれば、鍵配送処理４０７で、制御部２は、再生装置鍵記憶部２０４内のので再生装置鍵を鍵記憶装置識別コード記憶部２０７の再生装置識別コードとともに制御部３０２に送信する。そして、履歴書き込み処理４０７で、コンテンツ識別コード記憶部２０８、再生装置識別コード記憶部２０９、時刻情報記憶部２１０の情報を履歴情報として記憶する。

【００２６】

図５は、履歴情報の記録例であり、図6は、その記録処理手順の説明図である。図６において、６０１は、開始処理、６０２は、鍵を利用していない期間を記録する未使用期間記録処理、６０３は、開始時刻を記録する開始時刻記録処理、６０４は、鍵使用終了時刻記録処理である。

【００２７】

以下処理を説明する。図５において、最初の1行目は、すでに書き込まれているものとする。これは、鍵の有効期間の開始時刻か書き込まれている。未使用期間記録処理６０２では、その時点で書き込まれている最終行の一番左の列の時刻情報を現在時刻の時間差を未使用時間として1列めに記録する。2列目には、最終

行の一番左の列の時刻情報を3列目は、現在時刻を記録する。そして、今書き込んだ行と一つ前の行のデータについての改ざん検出用のハッシュ処理を行い4列目に記録する。

【００２８】

次に、開始時刻記録処理６０３は、現在時刻を1列目に、2列目に再生装置識別コード、3列目にコンテンツ識別コードを記録し、さらに今書き込んだ行と一つ前の行のデータについての改ざん検出用のハッシュ処理を行い4列目に記録する。

【００２９】

次に、制御部３０３が取得した再生装置鍵の使用を終了したことを示す信号として時刻情報を送信したとき、制御部２２は、鍵使用終了時刻記録処理を行う。これは、送られてきた終了時刻を1列目に、2列目に再生装置識別コード、3列目にコンテンツ識別コードを記録し、さらに今書き込んだ行と一つ前の行のデータについての改ざん検出用のハッシュ処理を行い4列目に記録する。

【００３０】

以上の処理により、履歴情報は、常に記録されるたびに直前の情報との改ざん検出コードでつながれるため、改ざん検出コードの生成方法が暴露されない限り、途中に不正な履歴を挟むと簡単にその位置が検出できる。そして記録去れるデータの最終行の1列めデータが最新の時刻情報であり、常にこの時刻よりも進んだ時刻が示されない限りられてきた値を記憶して、最新読み取り時刻との比較処理４０４で処理を中止されてしまうので、時刻情報を逆に進ませる不正を防止できる。また、鍵に取得時刻に加えて終了時刻まで記録した場合には、少なくともその再生時間分は、時刻を進ませることができるので時刻の不正を働いてもその再生できる時間は高々完全に連続再生している場合より長くはできない。また、履歴記憶部の容量を有限の値にしておけば、その記憶量いっぱいに履歴が書き込まれるとそれ以上履歴が書き込めないので処理が不成功となり鍵配送されなくなるため、記憶容量によって鍵取得回数の上限を制限できる。

【００３１】

図７は、図５のように記録された履歴が電子透かし情報の読み出し処理に利用

する場合の説明図である。図７において、７０１は、不正に複製された記録メディア、７０２は、電子透かし情報検出装置、７０３は、再生装置識別コードによる検索検証処理、７０４は、鍵記憶装置識別コードによる検証処理、７０５は、鍵取得時刻情報による検証処理である。電子透かし情報検出処理７０２で検出された埋め込み情報は、不正者により改ざんされている可能性がある。すなわち、不正を働いたものは、埋め込み情報による追跡から逃れるためにに埋め込み情報の削除や改ざんを試みることが想定される。その結果、埋め込み部分を抜き取る事による情報の欠損や、でたらめなデータの埋め込みによる改ざんへの試みによる一部のデータの誤検出が考えられる。そこで、埋め込まれた情報のどれか一つでも正しく検出されていた場合には、鍵記憶装置に貯えられた履歴を回収する事でできる履歴データベースを検索することで残りの情報を復元できる。再生装置識別コードによる検索検証処理７０３、鍵記憶装置識別コードによる検証処理７０４、鍵取得時刻情報による検証処理７０５でそれぞれの情報から残りの情報を復元できる。またこれらの情報ををまとめて、それと最も相関性の高いものを履歴情報から見つける事でもかなり高い確率で不正を行ったデータ再生装置や鍵記憶装置や犯行時刻等が推定できる。

【００３２】

図８は、電子透かし情報埋め込み手段１１あるいは３０８の構成とその検出装置の構成の説明図である。図８において８０１は、埋め込みシーケンス生成部、８０２は、映像1フレームに情報埋め込み処理する電子透かし埋め込み処理部、８０３は、短周期埋め込みパターン検出部、８０４は、長周期埋め込みパターン検出部、８０５は、電子透かし検出部である。以上の構成において以下にその動作を説明する。埋め込みパターンとして、機器識別コード、鍵記憶装置識別コードや時刻情報を含んだビットパターンが代入される。入力されたビットパターンは、埋め込みシーケンス生成部８０１で各映像フレームに埋め込むパターンの列に変換され、各フレーム毎に電子透かし埋め込み処理部８０２に送られる。埋め込みシーケンス生成部では、入力された埋め込みパターンを1フレーム当たりに埋め込めるビット数に応じて分割して各フレームへの埋め込みパターンとする。たとえば、簡単のために埋め込みパターンが８バイトで1フレーム当たり4ビット

を埋め込み処理する場合、埋め込みパターンが“０１１００１０１１１００１０１０”ならば、各フレームには、順に１６進数で“６５ｃａ”を最初の４フレームに埋め込む。次に、今の埋め込みパターンと同じフレーム数の映像に埋め込みパターンの第一ビットパターンである“０”を入力する。次に、先程入れたパターンと同じフレーム長間、埋め込みパターンの先頭ビット値を埋め込み値として埋め込む。すなわち、埋め込み値が０のときは、４フレーム間０を、１の場合は、４フレーム間１６進数でＦＦＦＦを出力する。次に再び最初に埋め込んだパターン“６５ｃａ”を順に埋め込み、次に埋め込み値の第２のビットを埋め込む。以上のように、埋め込みパターンを順に埋め込み次にそれと同じ長さの期間内に１ビットだけ埋め込むことを順に繰り返す。すなわち、順に埋め込んだ短周期の埋め込みとそのビット数倍の長周期に繰り返す埋め込みパターン列を生成する。図９は、その埋め込み処理の結果、各フレームに埋め込まれるパターン列を説明した図である。電子透かし埋め込み処理部８０２では、各フレームごとに入力されるパターンにそって情報埋め込み処理して、埋め込み情報つきデータとする。検出の場合は、電子透かし情報検出部８０５で各フレーム毎の埋め込みパターンを検出する。本実施の形態では、原画像を参照画像として用いているが、参照画像なしで検出できる埋め込み方式の場合原画像を参照しなくてもよい。各フレームの埋め込みパターン検出結果は、短周期埋め込みパターン検出部８０３、長周期埋め込みパターン検出部８０４へ送られる。短周期埋め込みパターン検出部８０３は、短周期に埋め込まれたビット列部分の検出結果を繰り返し、比較し各ビットで最も出現回数が多い方のビット値として検出値とする。長周期埋め込みパターン検出部８０４は、各ビットの埋め込み期間内での検出結果、たとえば、図９における第５フレームから第８フレームまでが、すべて１かあるいは０であるかを検出する。両方の値がすべて同じでない場合、より多くのビット値を示す側の値とする。以上の処理の埋め込みパターンでは、できるだけ高い密度で埋め込んでいるのでわずかなフレームで電子透かし情報が解読できる。また、長周期的に１ビットずつ検出するため、少しの電子透かしを改ざんしても多数決判定することで求める事ができる。そして、各ビットの判定を埋め込みパターン分判定することで埋め込みパターンを求めることができる。したがって、短周期で埋め込

んだ場合、映像中の数フレーム毎に埋め込み情報があるため、映像データを編集されたりしても検出できるが一方でフレームを抜き取るなどの改ざんに弱い。一方、長周期に埋め込んだ場合、長い期間の映像データを検出しないと埋め込みパターンが検出できないがフレームを抜き取るなどの攻撃に強いため、２つの埋め込みパターンを併用することで弱点を補いあった改ざんや編集につよい埋め込み方法が実現できる。なお、長周期と短周期の併用しかたであるが本実施例以外のやり方でも同様の効果が期待できる。たとえば、１フレームに４ビット埋め込むとしてそのうち３ビットを短周期の埋め込み様に１ビットを長周期の埋め込み様に用いて両方を並列に埋め込むことも出来る。

【００３３】

以上示したように本実施の形態のデータ再生装置によれば、鍵記憶装置にその鍵への読み取り履歴を記録しているため、有効期限確認等で現在の時刻を偽って申告しようと試みた場合でもかならず時計を進める方向にしか鍵を受け取れる時刻はないので不正が出来たとしても高々常に再生しつづけた場合に再生できる再生時間以上に再生させることが出来ない様に出来る。また、鍵記憶装置の履歴記録部分の容量は有限なので、履歴容量を越えて鍵を取得することはできないので不正回数の上限を制限できる。

【００３４】

また、履歴についてもハッシュ値をつけることにより改ざんが困難な履歴書き込みが実現できる。

【００３５】

さらに、本実施の形態によれば、鍵記憶装置に記録した履歴で埋め込みデータの検出精度をあげることが出来るし、また、埋め込み情報で検出した結果との照合は、より確かな不正の証拠を示すことが出来る。

【００３６】

さらに情報埋め込みパターンとして短周期と長周期に２つの方法を併用して埋め込むため、改ざんにつよい埋め込み方法が実現できる。

【００３７】

なお、鍵記憶手段が鍵の読み出しの際、鍵の有効期間などのチェックを行った

が、データ再生装置が耐タンパ性が保証されていて改造されないのであれば、鍵記憶装置から鍵情報や履歴情報を暗号通信で受け取り、それに基づきデータ再生装置側で判定させる構成を撮ることも出来る。この場合は、履歴情報もデータ再生装置側で作成し鍵記憶装置に暗号通信して記録させることもできる。

【００３８】

また、図４の前回アクセス時刻チェックにおいて、履歴情報から時刻情報ｗお取り出す際、図５のハッシュ値を用いて履歴データ自身が改ざんされていないかどうか確認させるとより安全性が向上する。すなわち履歴情報中からハッシュ値を計算した場合と同じ処理をしてハッシュ値との一致を調べることで改ざんチェックが実現できる。

【００３９】

また、本実施の形態では、履歴に際して鍵の取得時の時刻、終了時の時刻、不使用の時刻と完全に連続した履歴を記録したが、単に、鍵へのアクセス時刻のみを記録しても時計を進ませる方向にしか動かせられない特徴はまた維持でき、本発明の効果を維持しているものである。

【００４０】

【発明の効果】

以上のように本発明（請求項１）によれば、有効期限付きの鍵についてその申告時刻を逆進させる不正を防止できる。

【００４１】

以上のように本発明（請求項２、１０）によれば、鍵取得履歴を改ざんするのが艱難な記録ができる。

【００４２】

また、以上のように本発明（請求項３）によれば、履歴情報の改ざんによる鍵の有効期間を越え不正使用を防止できる。

【００４３】

また、以上のように本発明（請求項４）によれば、鍵へのアクセスの上限値を制限できる。

【００４４】

また、以上のように本発明（請求項５、６、７，８，９）によれば、記録された履歴情報と透かし情報を突き合わせることができるため、不正者への追跡制をより高くすることが出来る。

【００４５】

また、以上のように本発明（請求項１１、１２）によれば、改ざんに強い透かし埋め込み装置と検出装置が実現できる。

【図面の簡単な説明】

【図１】

本発明の実施の形態のデータ再生装置および鍵記憶装置を含むシステムの構成図

【図２】

本発明の実施の形態の鍵記憶装置２の構成図

【図３】

本発明の実施の形態の再生システムの別の構成を示す図

【図４】

本発明の実施の形態の再生装置鍵取得処理の処理手順の説明図

【図５】

本発明の実施の形態の履歴情報の記録例の説明図

【図６】

本発明の実施の形態の記録処理手順の説明図

【図７】

図５のように記録された履歴の電子透かし情報の読み出し処理の説明図

【図８】

本発明の実施の形態の電子透かし情報埋め込み手段１１あるいは３０８の構成とその検出装置の構成の説明図

【図９】

本発明の実施の形態の各フレームに埋め込まれるパターン列を説明する図

【符号の説明】

１　鍵管理部

２　鍵記憶装置
３　再生装置鍵記憶部
４　有効期間記憶部
５　履歴記憶部
６　鍵記憶装置識別コード記憶手段
７　データ再生装置
８　データ再生装置識別コード記憶部
９　鍵複号処理部
１０　再生処理部
１１　電子透かし埋め込み処理部
１２　時計
１３　記録メディア
１４　鍵暗号化手段
１５　情報埋込装置
２０１　入出力インターフェイス
２０２　制御部
２０３　履歴情報記憶部
２０４　再生装置鍵記憶部
２０５　有効期間記憶部
２０６　鍵記憶部再生装置間鍵記憶部
２０７　鍵記憶装置識別コード記憶部
２０８　コンテンツ識別コード記憶部
２０９　再生装置識別コード記憶部
２１０　時刻情報記憶部
３０１　入出力インターフェイス部
３０２　制御部
３０３　鍵記憶装置識別コード記憶部
３０４　再生装置識別コード記憶部
３０５　鍵取得時刻記憶部

３０６　鍵復号処理部

３０７　再生処理部

３０８　電子透かし情報埋め込み処理部

３０９　コンテンツ識別コード記憶部

３１０　鍵記憶部再生装置間鍵記憶部

４０１　コンテンツ識別コード取得処理

４０２　時刻情報取得処理

４０３　鍵リクエスト送信処理

４０４　最新読み取り時刻との比較処理

４０５　鍵有効期間確認処理

４０６　履歴書き込み処理

４０７　鍵配送処理

６０１　開始処理

６０２　未使用期間記録処理

６０３　開始時刻記録処理

６０４　鍵使用終了時刻記録処理

７０１　不正に複製された記録メディア

７０２　電子透かし情報検出装置

７０３　再生装置識別コードによる検索検証処理

７０４　鍵記憶装置識別コードによる検証処理

７０５　鍵取得時刻情報による検証処理

８０１　埋め込みシーケンス生成部

８０２　映像1フレームに情報埋め込み処理する電子透かし埋め込み処理部

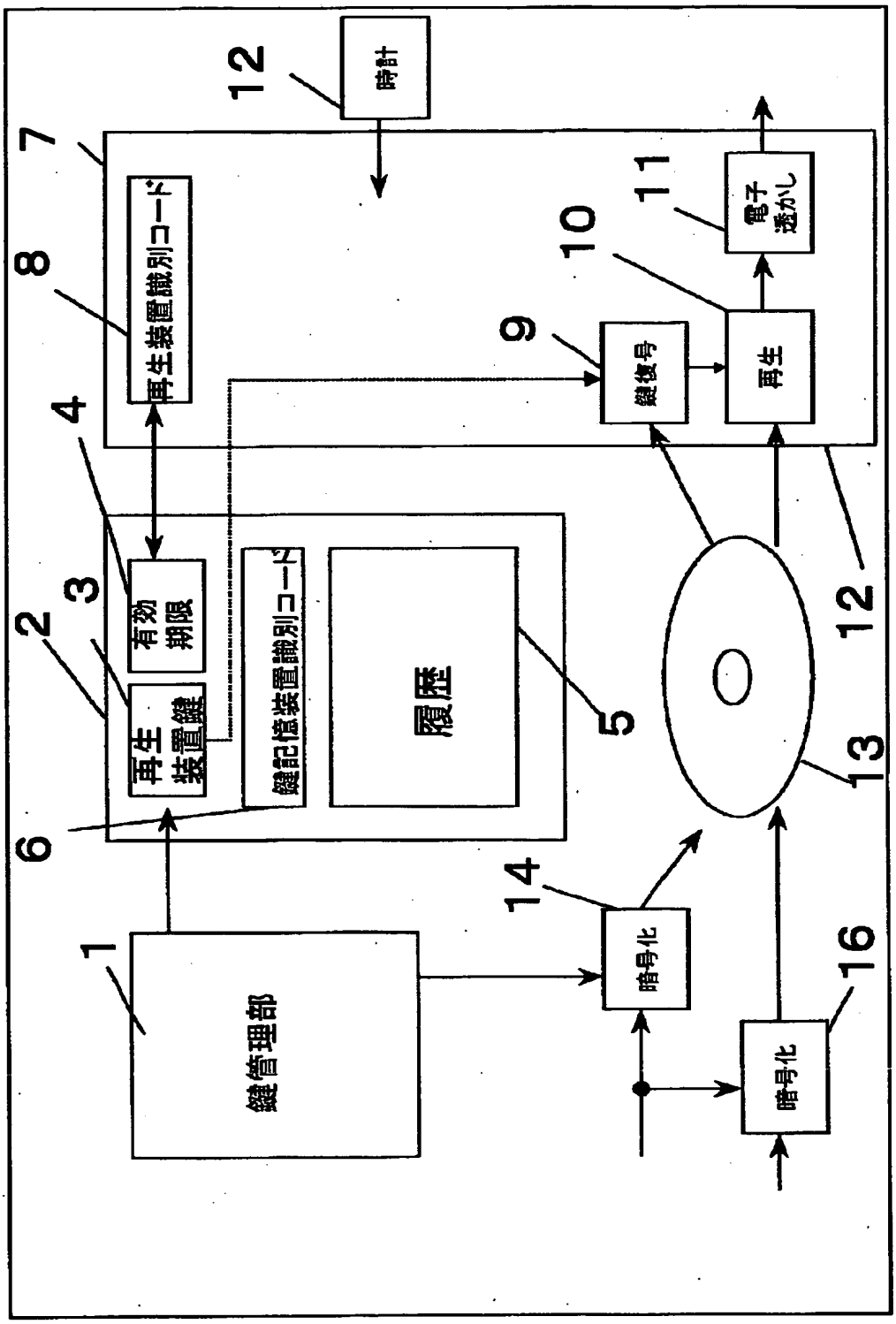
８０３　短周期埋め込みパターン検出部

８０４　長周期埋め込みパターン検出部

８０５　電子透かし検出部

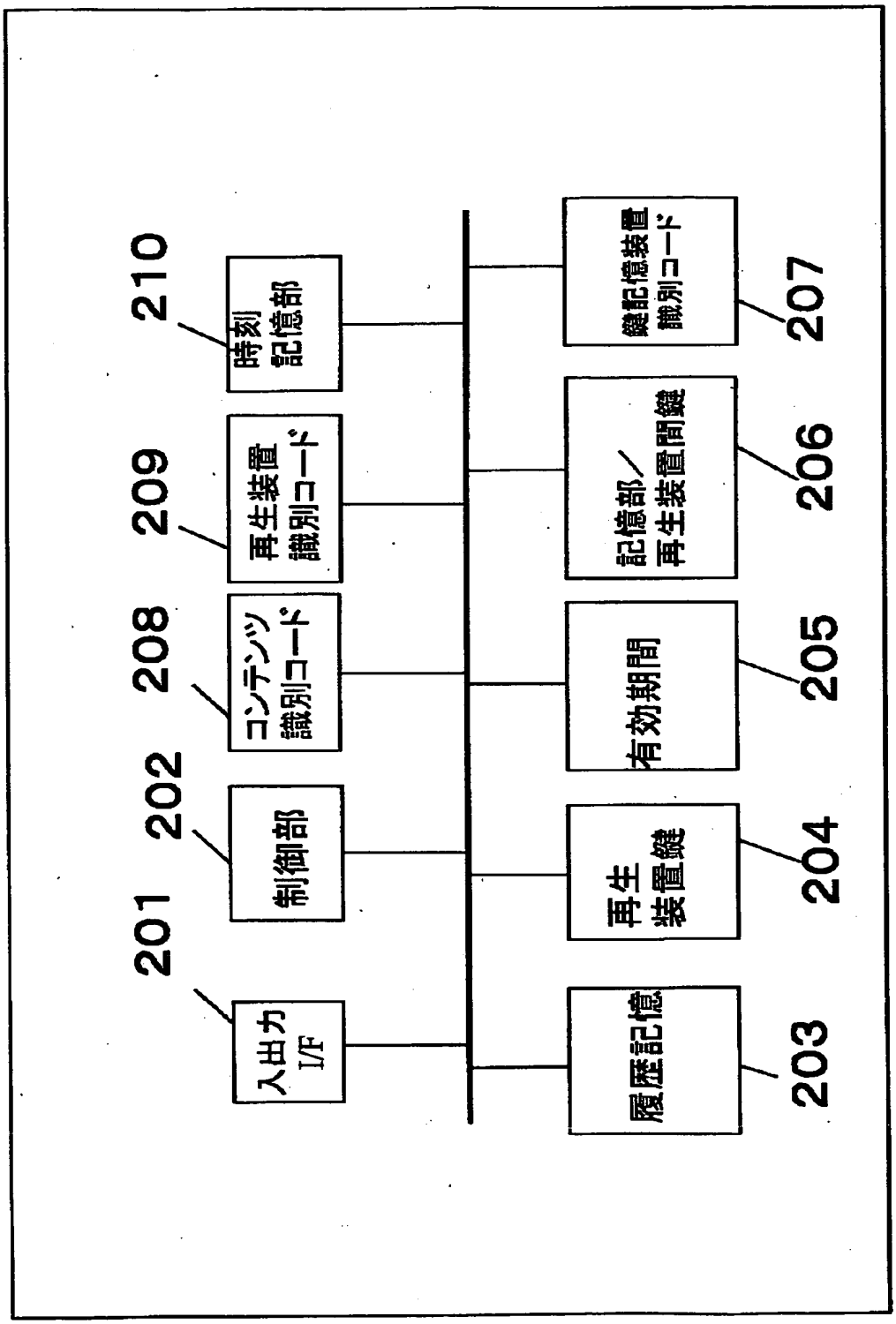
【書類名】　　図面

【図１】

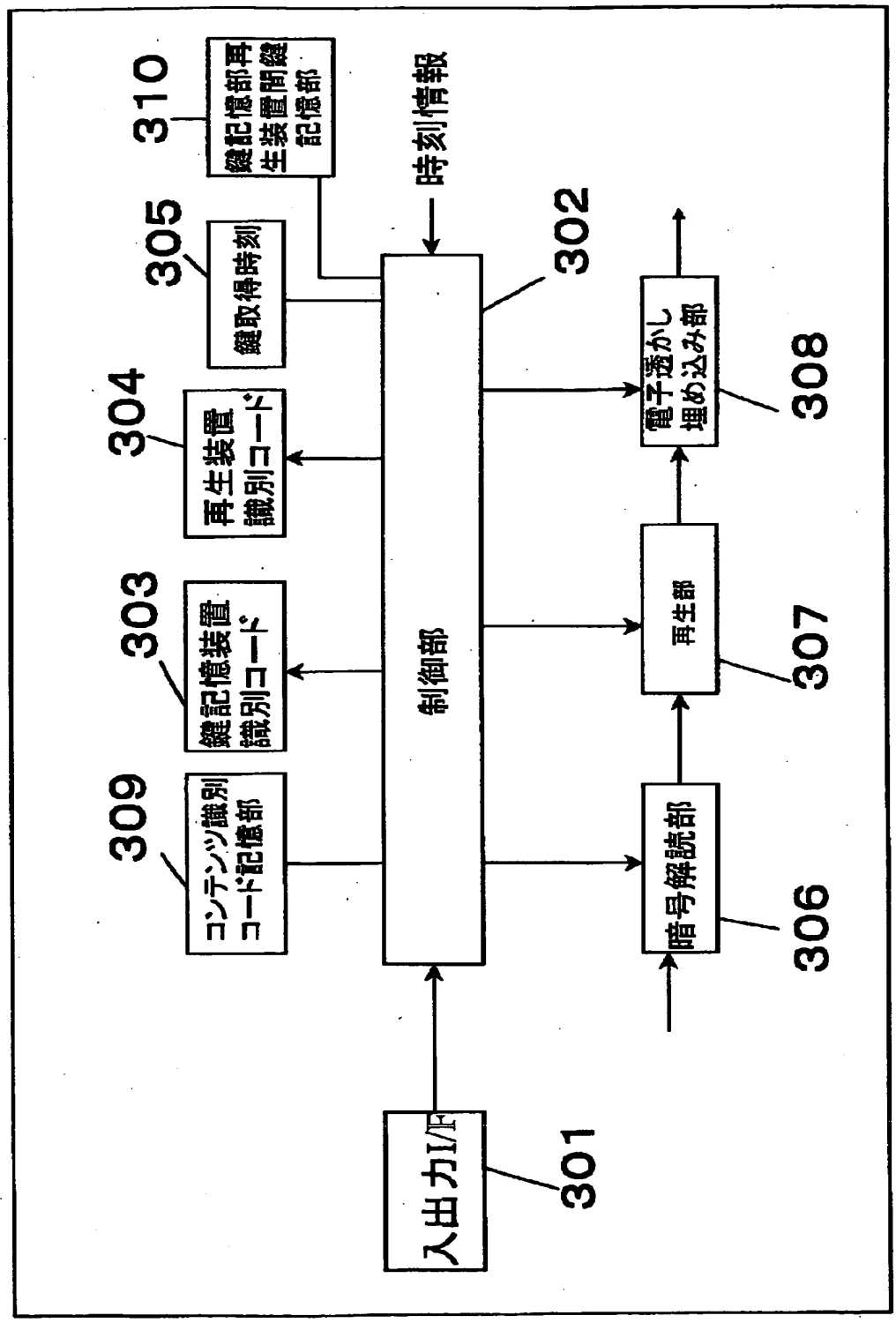


出証特２０００－３０４４８５６

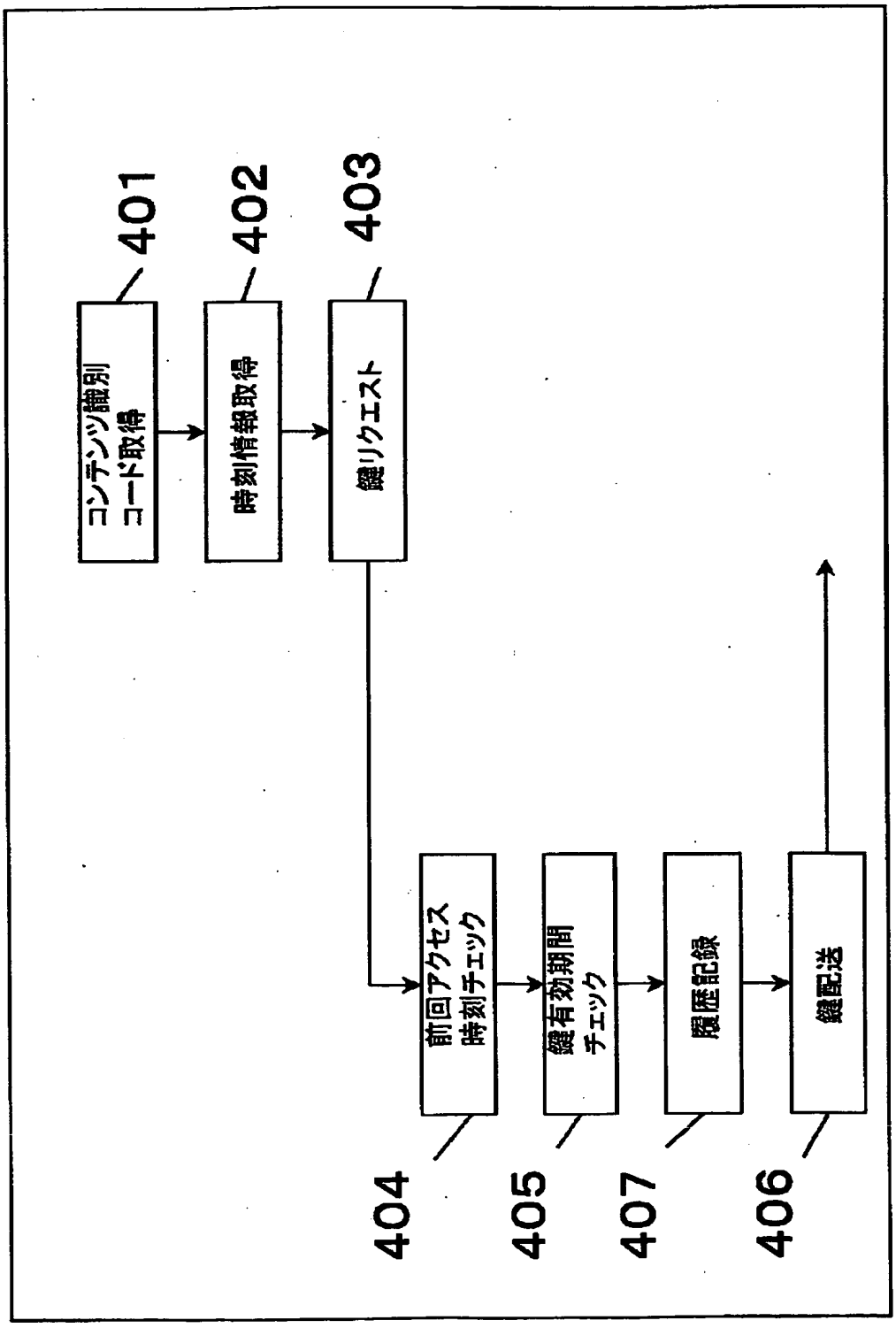
【図２】


201
入出力 I/F
202
制御部
208
コンテンツ識別コード
209
再生装置識別コード
210
時刻記憶部
203
履歴記憶
204
再生装置鍵
205
有効期間
206
記憶部／再生装置間鍵
207
鍵記憶装置識別コード

【図３】


310
鍵記憶部再生装置間鍵記憶部
時刻情報
305
鍵取得時刻
302
304
再生装置識別コード
電子透かし埋め込み部
308
303
鍵記憶装置識別コード
制御部
再生部
307
309
コンテンツ識別コード記憶部
暗号解読部
306
入出力I/F
301

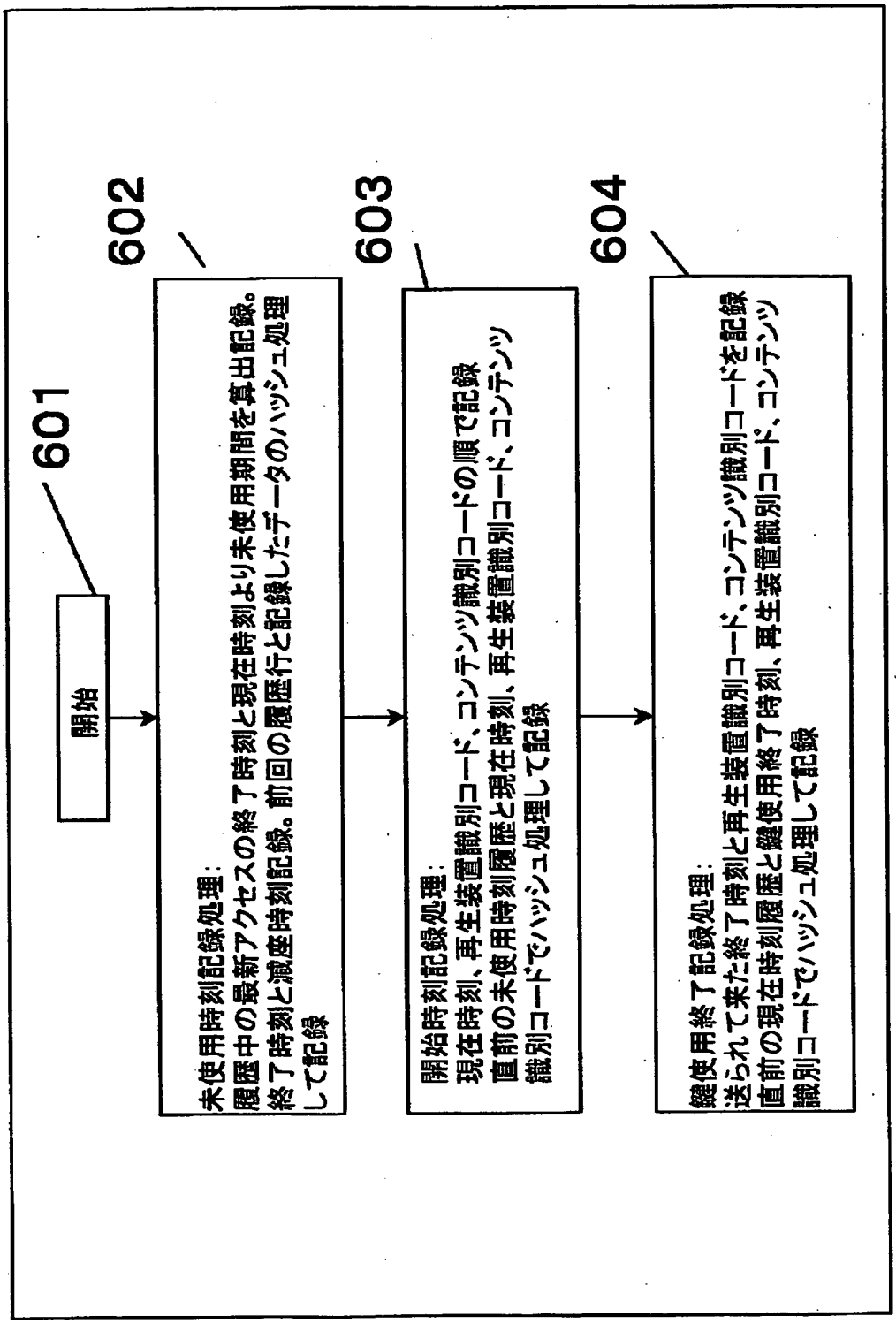
【図４】


401
402
403
コンテンツ識別コード取得
時刻情報取得
鍵リクエスト
前回アクセス時刻チェック
鍵有効期間チェック
履歴記録
鍵配送
404
405
407
406

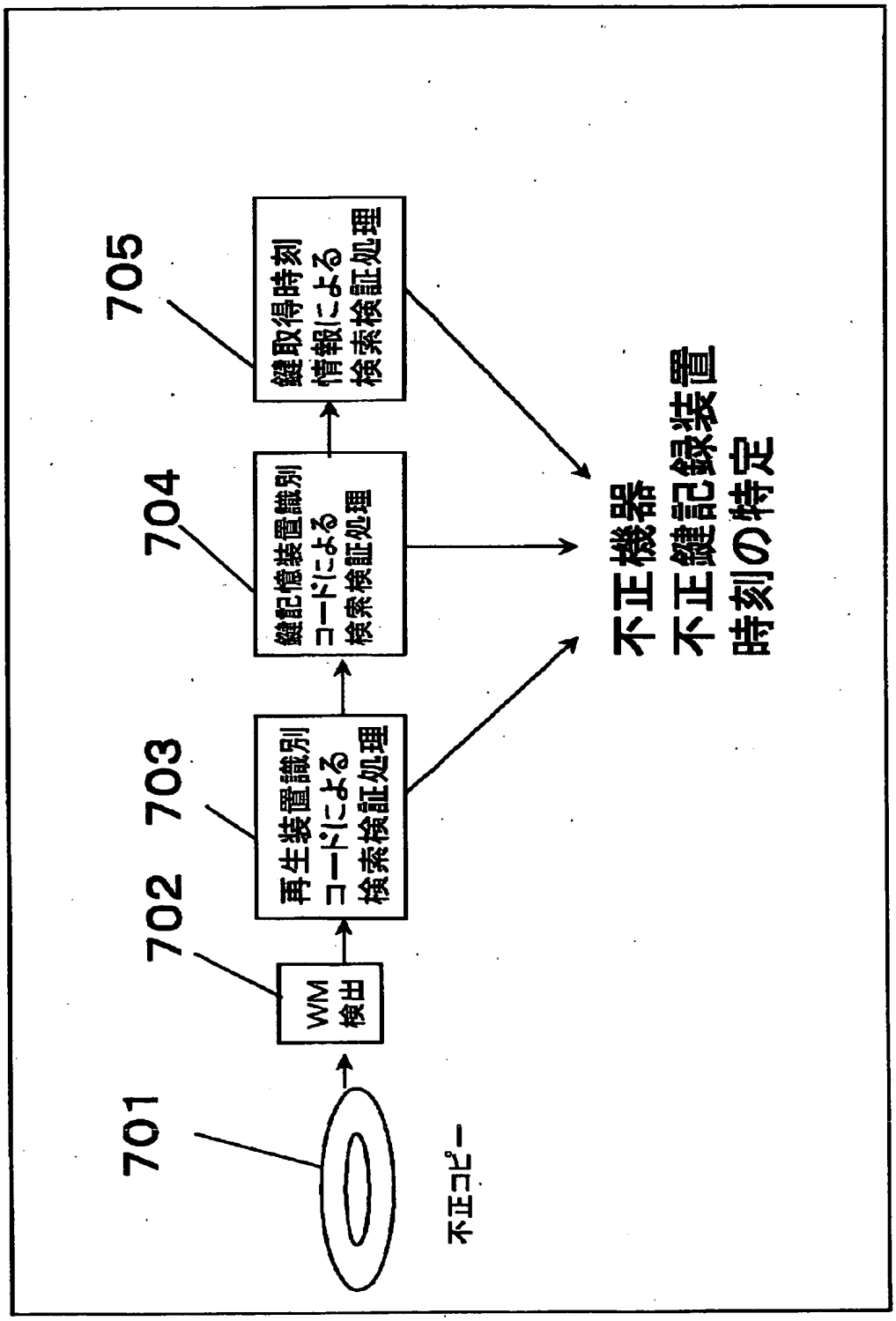
【図５】


鍵有効時刻
ハッシュ値1
未使用期間
鍵有効時刻
開始時刻1
ハッシュ値2
開始時刻1
再生装置識別コード1
コンテンツ識別コード1
ハッシュ値3
終了時刻1
再生装置識別コード1
コンテンツ識別コード1
ハッシュ値4
未使用期間
終了時刻1
開始時刻2
ハッシュ値5
開始時刻2
再生装置識別コード1
コンテンツ識別コード2
ハッシュ値6
終了時刻
再生装置識別コード2
コンテンツ識別コード2
ハッシュ値7

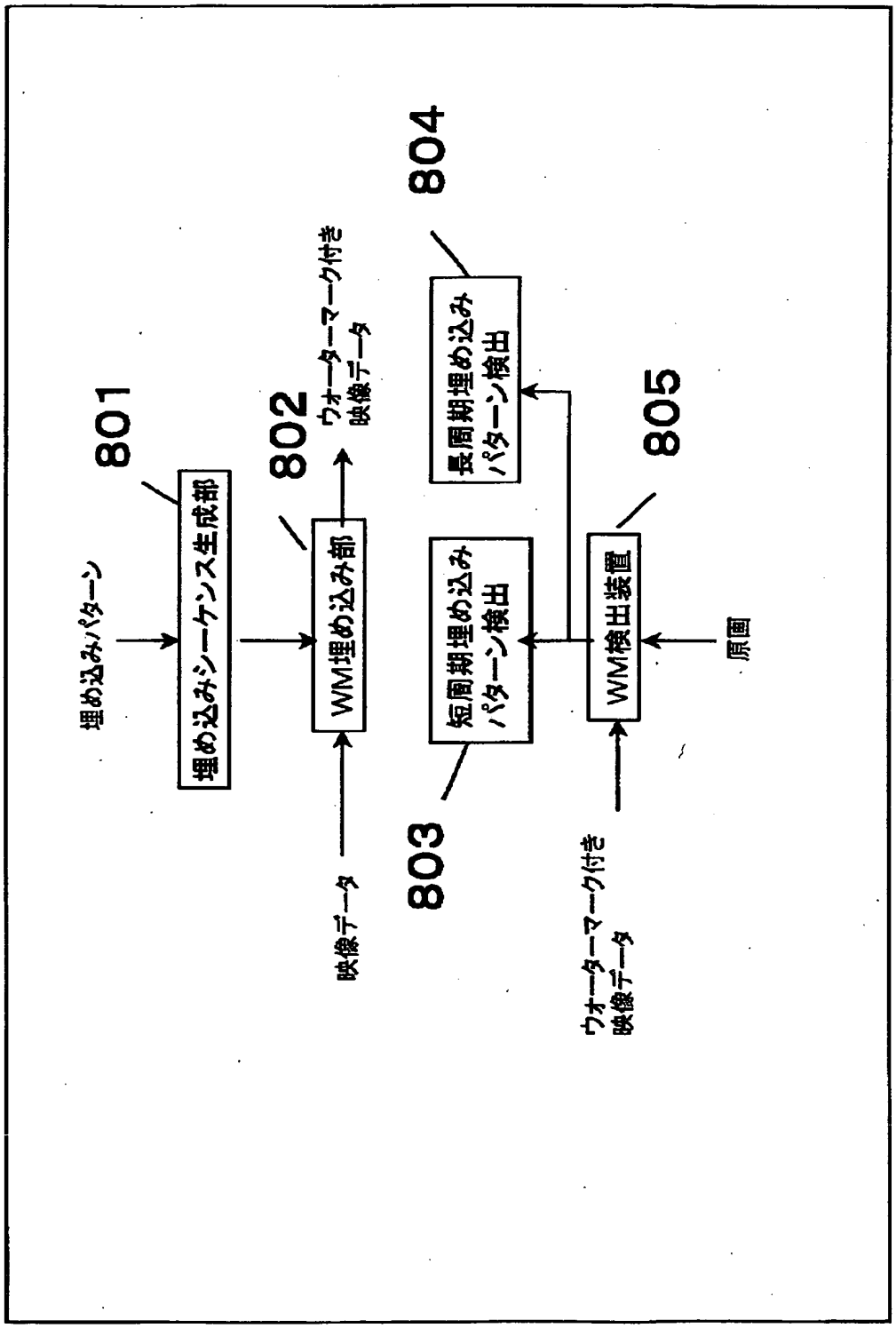
【図６】


601
開始
602
未使用時刻記録処理：
履歴中の最新アクセスの終了時刻と現在時刻より未使用期間を算出記録。
終了時刻と減座時刻記録。前回の履歴行と記録したデータのハッシュ処理
して記録
603
開始時刻記録処理：
現在時刻、再生装置識別コード、コンテンツ識別コードの順で記録
直前の未使用時刻履歴と現在時刻、再生装置識別コード、コンテンツ
識別コードでハッシュ処理して記録
604
鍵使用終了記録処理：
送られて来た終了時刻と再生装置識別コード、コンテンツ識別コードを記録
直前の現在時刻履歴と鍵使用終了時刻、再生装置識別コード、コンテンツ
識別コードでハッシュ処理して記録

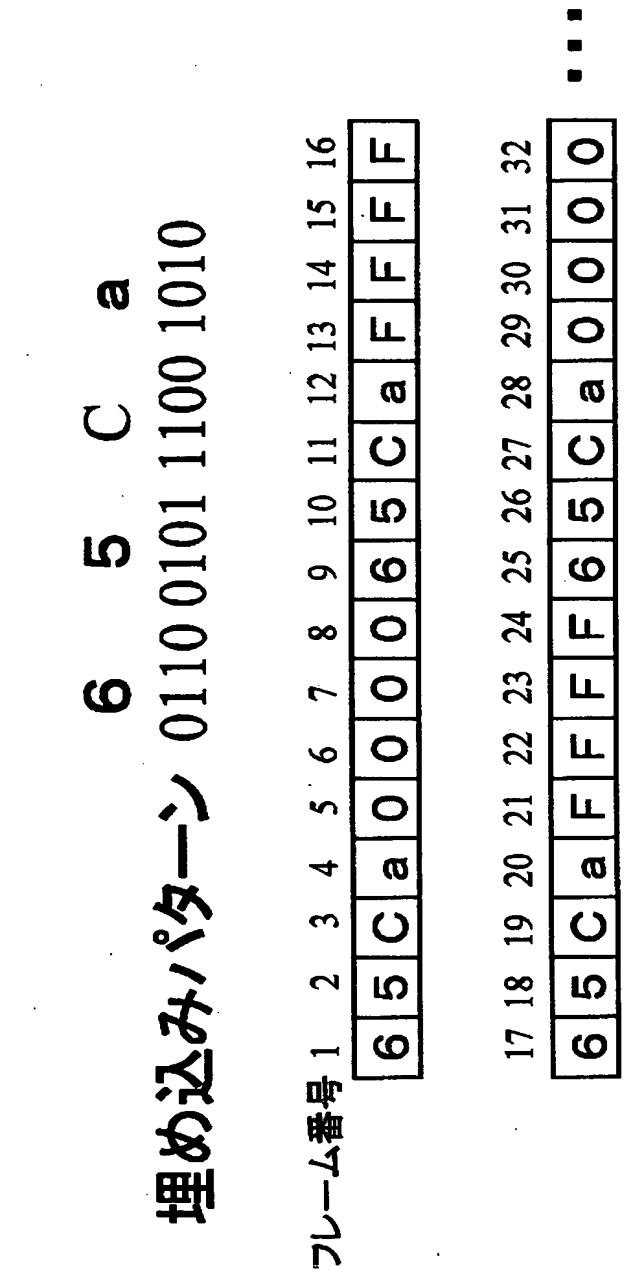
【図７】


701
不正コピー
WM
検出
702
再生装置識別
コードによる
検索検証処理
703
鍵記憶装置識別
コードによる
検索検証処理
704
鍵取得時刻
情報による
検索検証処理
705
不正機器
不正鍵記録装置
時刻の特定

【図８】


801
埋め込みパターン
埋め込みシーケンス生成部
802
WM埋め込み部
ウォーターマーク付き
映像データ
804
最周期埋め込み
パターン検出
805
WM検出装置
原画
803
短周期埋め込み
パターン検出
映像データ
ウォーターマーク付き
映像データ

【図９】


埋め込みパターン 0110 0101 1100 1010
6 5 C a
フレーム番号
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
6 5 C a 0 0 0 0 6 5 C a F F F F
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
6 5 C a F F F F 6 5 C a 0 0 0 0
...

【書類名】　要約書

【要約】

【課題】　再生限定するコンテンツ再生において有効期限付きで再生をするときの時刻情報の改ざんの防止と不正機器の精度の高い追跡性を実現する。

【解決手段】　再生用の鍵を運ぶ鍵記憶手段２に鍵へのアクセス履歴を記録していき、再生毎にその時刻と機器からの時刻を比較する。また、透かし情報と履歴情報を比較して追跡性を高める。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社